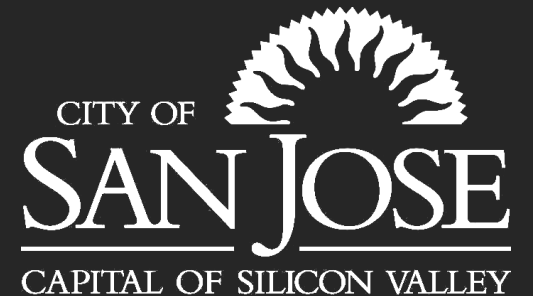


City of San José Digital Privacy Implementation

Rob Lloyd, Chief Information Officer
Marcelo Peredo, Chief Information Security Officer

September 2, 2021

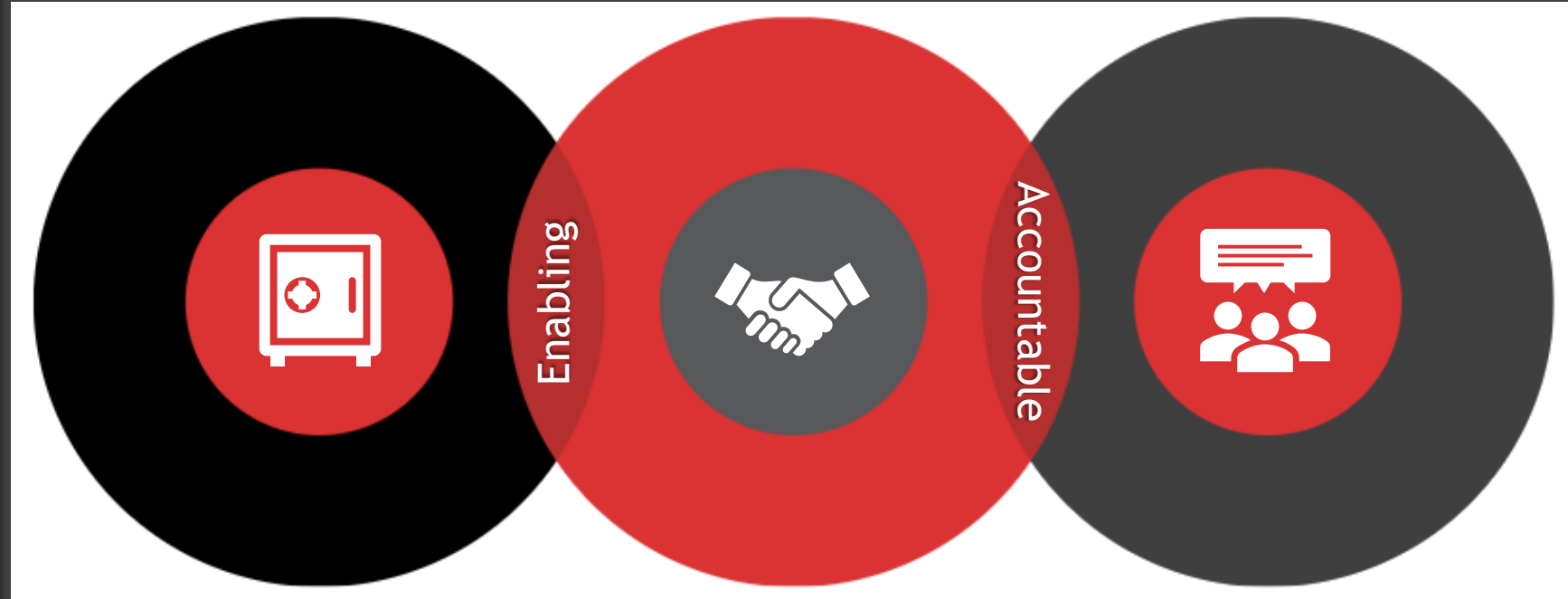


Digital Privacy Policy Implementation Status Report.

(Information Technology/Finance/City Attorney)

Purpose: Provide a status report on the Digital Privacy Policy implementation, including review, engagement, and technical protocols.

Status Updates



Security

Privacy = Trust

Engagement





San José is moving towards a data privacy model for secure, civic-minded data use.

2018 Privacy Principles

The following digital privacy principles were approved by the San José City Council on September 17, 2019, and reflect the input of stakeholders. These principles guide work in the City as we protect the data of our residents from new risks and keep the trust of our community.

WE VALUE PRIVACY: We affirm that privacy is an inherent human right. San José commits to fully evaluating risks to your privacy before collecting, using, or sharing your information.

WE COLLECT ONLY WHAT WE NEED: We collect only what is required to provide and improve city services and comply with the law. We seek community input about what information is used and collected.

WE ARE OPEN AND TRANSPARENT: We are transparent about what information we collect, why we collect it, and how it is used. We commit to being open about our actions, policies, and procedures related to your data. We make our policy documents publicly available and easy to understand.

WE WILL GIVE YOU CONTROL OVER YOUR DATA: We will provide you with the information to make an informed decision about sharing your data. We have clear processes that ensure data accuracy and provide you visibility into what data the city has collected from you.

WE SHARE ONLY WHAT WE NEED: We anonymize your information before we share it outside the city, except in very limited circumstances. Business partners and contracted vendors who receive or collect personal information from us or for us to deliver city services must agree to our privacy requirements.

WE DESIGN FOR PRIVACY AND SECURITY: We integrate privacy and security into every aspect of our designs, systems, and processes. We commit to updating our technology and processes to effectively protect your information while under our care. We follow strict protocols in the event your information is compromised.

2020 Privacy Policy

PURPOSE

...**safeguard the public's trust** in the City's use of new and emerging technologies and to protect their digital privacy rights

...**framework for City departments** to observe when information systems or other applications and forms collect the public's Personally Identifiable Information (PII)

...to the extent practicable, to **enable residents to determine** for themselves when, how and to what extent information about them is communicated to others

...**enable the City to harness the power of... insights** to provide better services to the community while ensuring that personal and sensitive information is properly protected

POLICY ELEMENTS

- **Notice** (Limited exceptions for Emergencies, Employer, Police, Fire)
- **Retention**
- **Minimization**
- **Accountability**
- **Accuracy**
- **Sharing**
- **Equity**

STAKEHOLDERS

- **CMO**: Resource Privacy Officer; Review/Approve Procedures; Budget
- **Departments**: Apply Policy Elements
- **ITD**: CISO = Data Security and Handling; Privacy Officer = Reviews/Practices + Outreach
- **Finance-Purchasing & CAO**: Procure Goods/Services; Contractual Requirements

EFFECTIVE: 7/1/2021 - <https://www.sanjoseca.gov/home/showpublisheddocument?id=68053>

City Council approved Privacy Policy in Dec 2020...

- Establishes expectations for **data usage transparency**
- Promotes data usage for advancing **city equity**
- Provides **safeguards for PII¹** while **supporting beneficial research** through data sharing
- Aligns SJ data practices with CA & USA laws + GDPR

...Council & residents voiced concerns on path forward

“I don’t want SJ to become real-life minority report”

“We need to anonymize data while not preventing policy-improving research”

“We’ve got to find a way to fund this going forward”

1. Personally Identifiable Information; SJ identifies 5 types of PII in its privacy policy: Personal, sensitive/demographic, image, recording, & geolocation
Source: San Jose data privacy policy & memorandums, SJ council meetings

Adopted Policy... with 2021 Backlogged Priority

Prioritized Backlog | FY 2021-2022

No.	Initiative/Policy Name (by points and alphabetized)	Points
1	Boost San José's Retail Sector (D1)	7
2	Update Council's Wage Theft Prevention Policy	7
3	Anti-Displacement Preference Ordinance	6
4	Local Hiring/Business/Apprentice Utilization Program	6
5	San José Surveillance Ordinance (D2) + Digital Privacy Policy Implementation	6
6	Traffic Calming Policy for Residential Neighborhoods	6
7	Urban Greening Implementation Plan	6
8	Universal Preschool Policy (D5)	5
9	Staffing Analysis (D7)	4
10	Universal Development Fee	4
11	Affordable Housing Construction Policy on City Land (D9)	3
12	Citywide Goals + KPI Dashboard (D10)	3
13	Private Percent for Art	3
14	Transit First Policy Framework	3

Source of Backlog Items	
Remaining, Unfinished FY 2020-2021 Council Policy Priorities [CP]	New Proposed FY 2021-2022 Council Policy Priorities [NP]
Referrals of Potential New Policies from FY 2020-2021 Rules Committee [RR]	Deprioritized FY 2020-2021 Enterprise Priority Initiatives [EP]

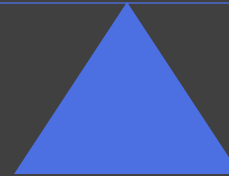
The Approach

“Privacy Light”

- Approved policy
- Not City Roadmap priority this tranche
- Significant future risk
- Practices in Data-Security-Tech
- Later maturity will require resourcing

Appropriate
Rigor

Speed



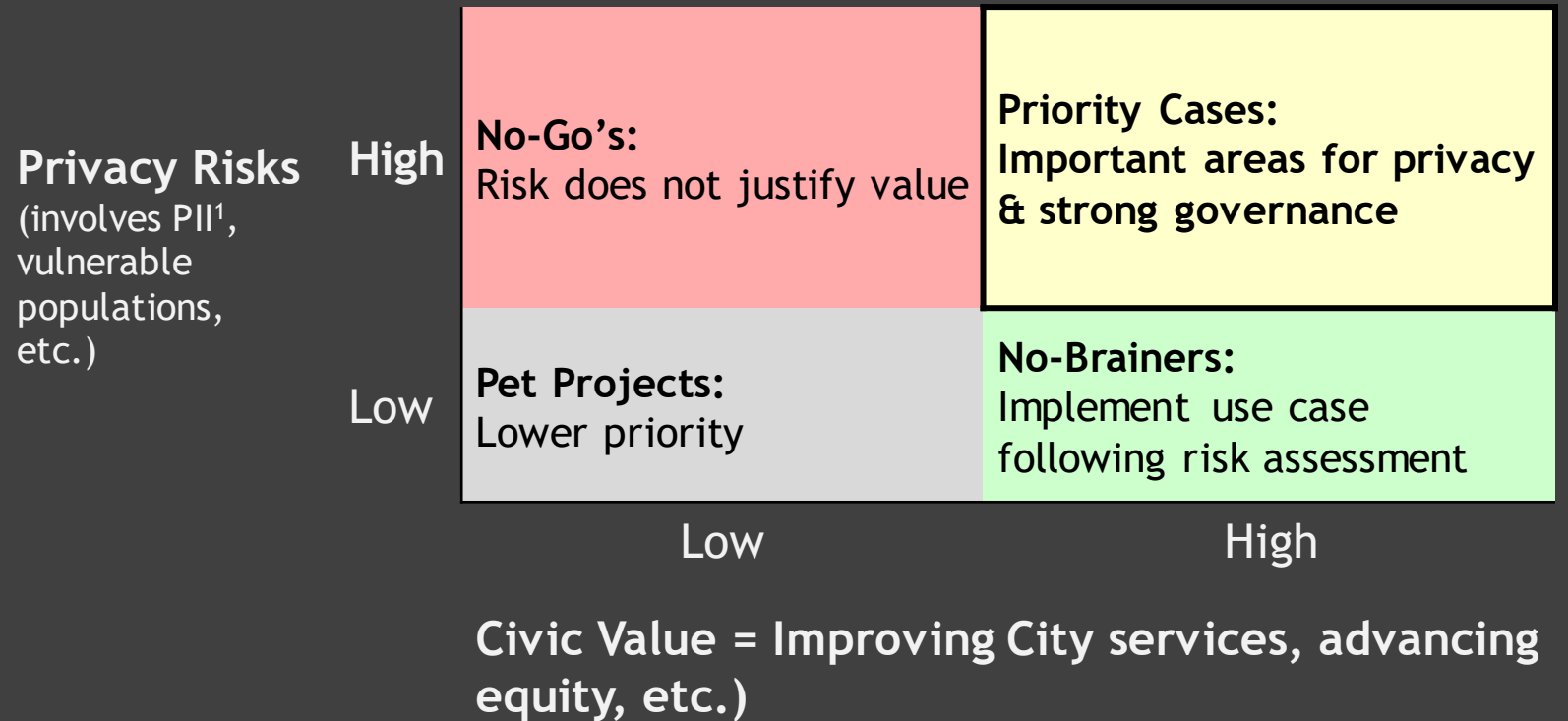
Processes

- Dept Notice/Outreach
- Tech/Security Review
- Procurement
- Budget and Legal Reviews
- Post-Use Reviews

Accelerators

- Contract Terms
- Standards
- Staffing
- Training/Support

Priority use cases are the intersection of high value & potential privacy risks



1. Personally Identifiable Information; SJ identifies 5 types of PII in its privacy policy: Personal, sensitive / demographic, image, recording, & geolocation
Source: San Jose data privacy policy & memorandums, SJ council meetings

Privacy Review Prior to Procurement

- Help Case
- Exhibit X
- Final Contract

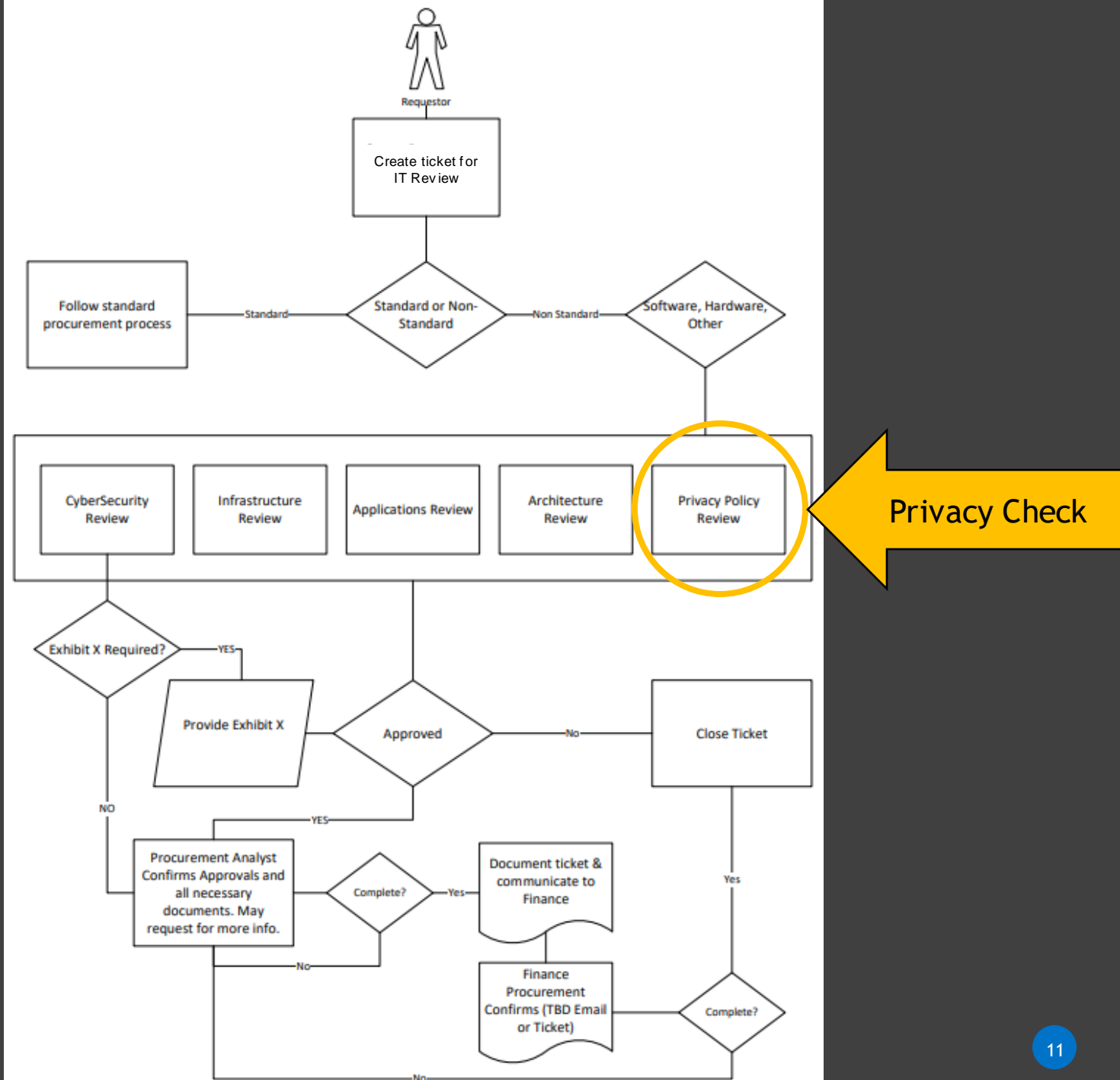


Exhibit X

EXHIBIT X:

INFORMATION TECHNOLOGY AND SECURITY REQUIREMENTS

The requirements checked below define the City's Information Technology and Security Requirements as they pertain to this Agreement. Contractor shall comply with the following requirements in providing all Information Technology-related software, services, and equipment.

☐ **1. Contractor's Software**

The terms for Contractor's Software licenses, including software accessed through a subscription service (Software), delivered pursuant to the Scope of Services, including subsequent Software updates licensed to the City, shall be as set forth in the Software License Agreement insert cross reference if applicable.

☐ **2. Non-Contractor Software**

Contractor shall procure, on City's behalf, the third-party software pursuant to and in accordance with the license and maintenance agreements insert cross reference if applicable. Contractor shall serve as City's agent for purposes of obtaining and implementing the items and services contemplated by such agreements. In procuring the third-party license and maintenance service, Contractor shall ensure the following:

- The license and service include guarantees and warranties;
- The City is either the direct or third party beneficiary to the guarantees and warranties of the agreement(s);
- The license and service include option(s) to purchase a warranty for a longer period if commercially available, and that the City may exercise the option(s);

☐ **3. Privacy and Disclosure**

Contractor agrees in the performance of services to comply with City's Privacy and Disclosure Policy, insert cross reference if applicable. Contractor shall ensure that all webpages that it creates are consistent with the Policy. Contractor further agrees that it shall treat all information received through the performance of this Agreement in strict accordance with the Policy.


Personal identifying information, financial account information, and restricted City information, whether in electronic format or hard copy, must be secured and protected at all times to prevent unauthorized access. At a minimum, Contractor shall encrypt and password-protect electronic files, store and process City data only in North America, and adhere to any applicable security standards, including the National Institute for Standards and Technology CSF/800-14/800-53/800-82, International Organization for Standardization 15408/27001/27002, International Society for Automation ISA-62443 series, Payment Card Industry PCI-DSS, Underwriters Laboratory, Health Insurance Portability and Accountability Act, Federal Risk and Authorization Management Program FedRAMP, U.S. Department of Justice/Federal Bureau of Investigation Criminal Justice Information Services Security Policy, et al., as may be amended or updated. This includes data saved to host locations, computers, connected devices, and storage devices.

☐ **4. Payment Card Industry Requirements**

Contractor agrees to comply with the City's Payment Card Industry (PCI) Requirements in the performance of the services provided under this Agreement insert cross reference if applicable.

☐ **5. Warranty for Services and Software Customizations**

Project Charters

Form Revision Date: 14 April 2021		Project Charter						
Privacy Review:	Notice	Retention	Minimization	Accountability	Accuracy	Sharing	Equity	
	Link to policy: https://www.sanjoseca.gov/home/showpublisheddocument?id=68053							

- Where digital privacy relevant, must identify and adhere to Policy
- Digital Privacy Officer will review and validate in the future

Digital Privacy Officer

Digital Privacy Officer

City of San Jose , California

JOB INFORMATION

Type

Full-Time

Department

Information Technology

Level

Senior Level

SALARY/WAGE

\$130,728.00 - \$159,993.60 Annually

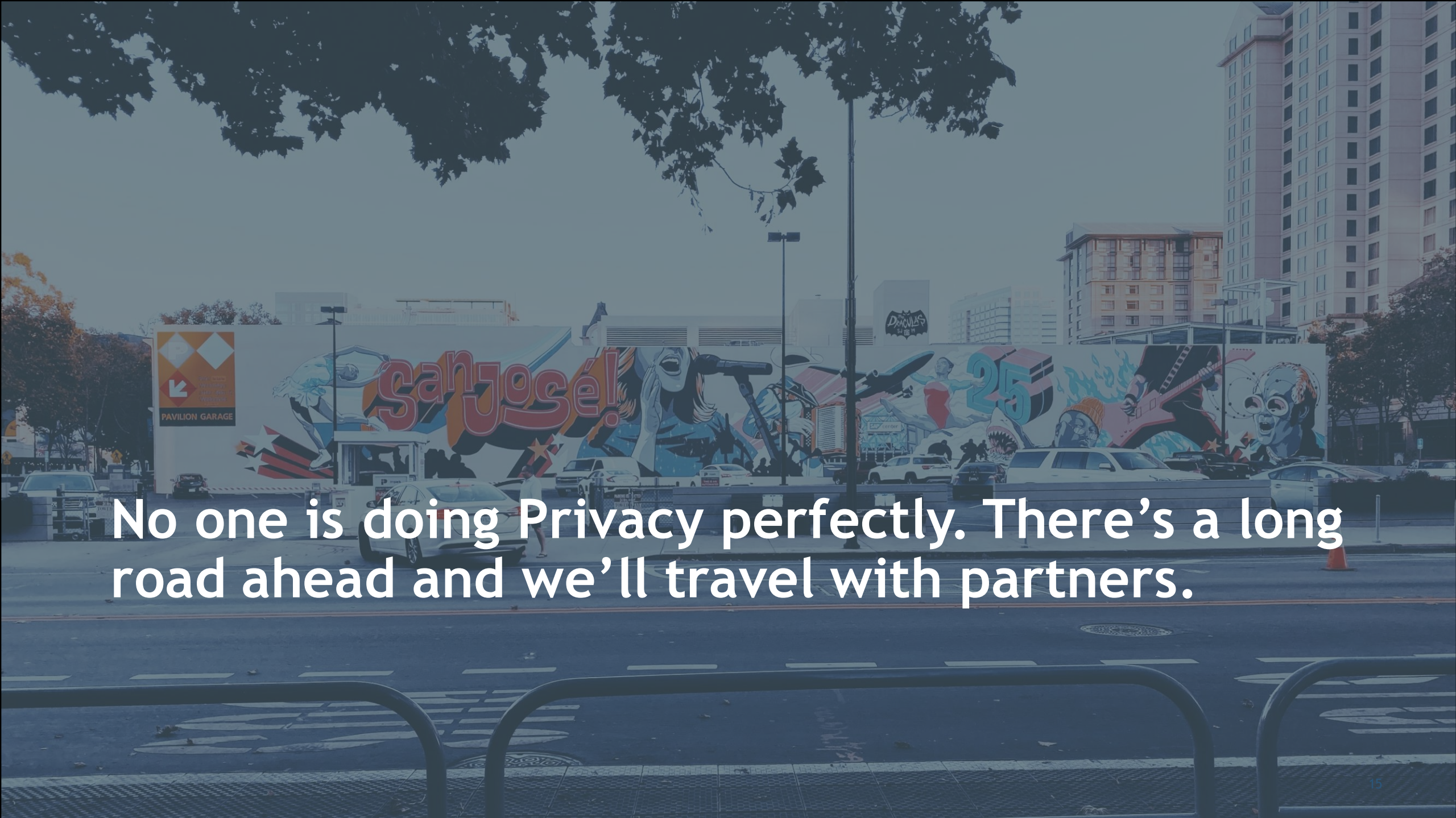
APPLICATION DEADLINE

1st Review June 29, 2021

RECRUITMENT TYPE

Open Competitive

- Full-time (FTE) position beginning FY21-22
- Focus on policy, practices, outreach
- Interview Panel with Advisory Board
- Posting highlights:
 - Works with internal and external stakeholders to **manage risks** tied to privacy laws, compliance, outreach, and emerging needs
 - Part of defining program structure that will serve to **operationalize Digital Privacy Policy**
 - Citywide **point-of-contact for privacy processes**
 - Will **partner** with City Attorney's Office, departments, and external partners in **administering the policy's** Notice, Retention, Minimization, Accountability, Accuracy, Sharing, and Equity elements



No one is doing Privacy perfectly. There's a long road ahead and we'll travel with partners.

15

State/Local Government Privacy Coalition

1. Working with Center for Digital Government
2. Charter for national effort to advance Digital Privacy practices in state/local government
3. Objects and Key Results + Survey being finalized

State/Local Government Privacy Coalition

KEY RESULTS

Model Work

- Model Digital Privacy Policy and Principles for rapid launch/adoption
- Digital Privacy Survey to collect current baseline of state/local government
- Privacy Resource Library online research repository of policies, work
- Model Privacy Officer Job Description

Education

- “Digital Privacy Basics” education guide including to help engage and educate constituents, elected/appointed officials, & staff on digital privacy
- Evolving and emerging privacy technologies map, frameworks, processes
- Updates on privacy legislation trends
- Establish a Digital Privacy community of practice

Privacy Products

- Create a Digital Privacy Review Tool and training that organizations can use
- Develop a capability maturity model and recommended baseline for state and local government
- Create a Digital Privacy Roadmap that outlines putting policy into practice
- Identify sponsors to support

State/Local Government Privacy Coalition

Survey

- Demographics
- Reporting Relationships
- Challenges/Concerns
- Current State of Digital Privacy Programs
- Organizational Privacy Assets in Place
- Priorities
- Measurement
- Topics of Interest

Advisory Task Force Feedback

1. City's Equity and Technology initiatives require a privacy focus, now.
2. Positive that concrete actions are being taken.
3. Cannot default sensor technologies to surveillance uses. Require protective reviews and assessments for those uses.
4. Build a practice knowledgebase of short case studies as a reference for projects- what was approved or denied and why, how the analysis was done.
5. Advisory Task Force members aim to give direct input and require concrete progress. Goal is not to be “window dressing”.
6. Coalition work to make Digital Privacy adoptable by and with peer cities is positive.



2021 Foundations |
2022 Practiced |
2023 Maturity |

Privacy is About the Trust of Our Community



Questions & Feedback

Appendix

Longer Road Ahead

Learning & Planning

FY21

- Continue community outreach & education
- Tweak privacy policy as needed per stakeholder input
- Identify FY22 funding for dedicated staff (i.e., Chief Privacy Officer)

Begin Risk & Impact Assessments— Policy Effective Date: 7/1/21

FY22

- Initiate inventory of data processing ecosystem, including data collection, cleaning, & usage
- Identify highest privacy concerns & opportunities for civic-minded data usage (“priority use cases”)
- Establish long-term funding for data privacy

Introduce GDPR governance & broaden scope

FY23

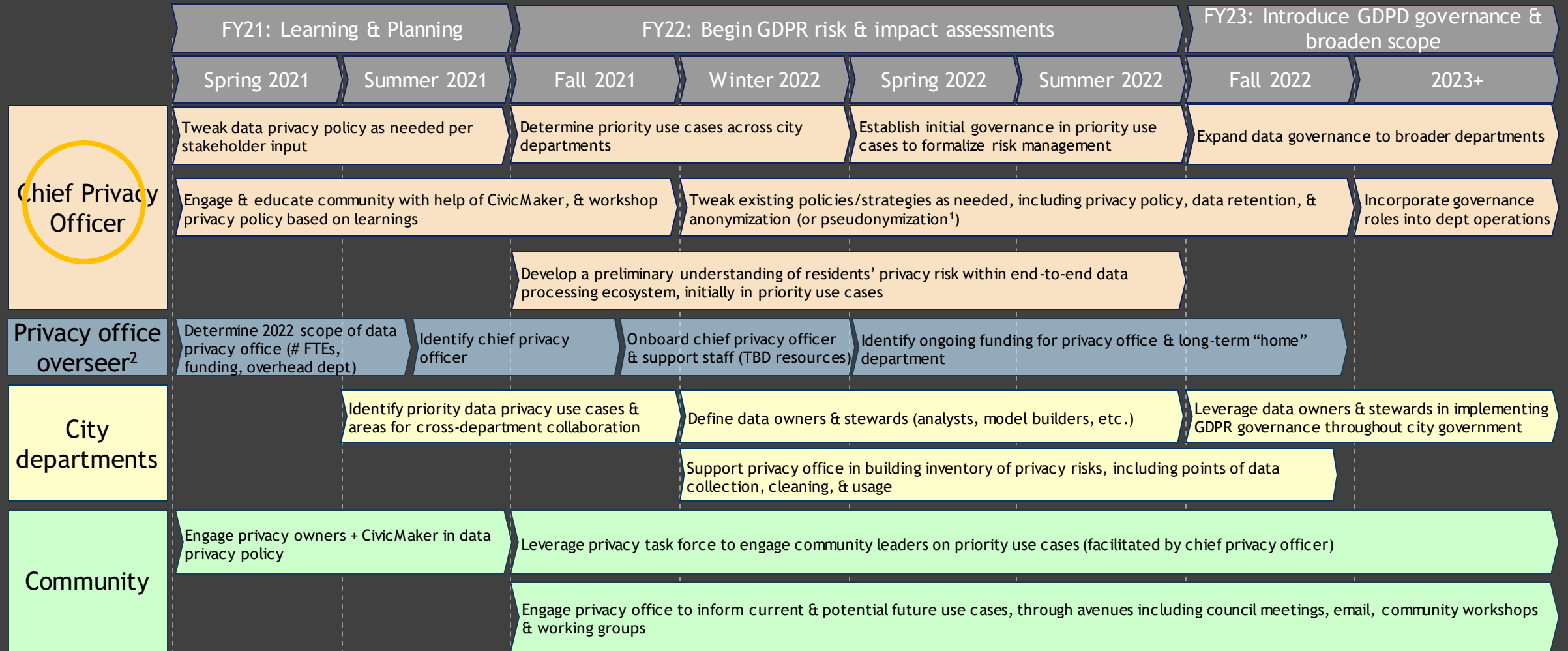
- Embed privacy governance in priority use cases
- Scale privacy policies/strategies beyond priority use cases

Establish full GDPR compliance

FY24+

- Apply privacy governance into city-wide practices
- Leverage secure ecosystem for further civic innovation

Detailed Roadmap: 2021 - 2023



1. Process of replacing sensitive data with identifier codes that enable merging datasets for cross-data insights (e.g., merging education & extracurricular data to identify after-school programs with positive educational impacts)

2. To be determined - department / umbrella office that the privacy office reports to